SECURING THE GLOBAL AIRSPACE SYSTEM VIA IDENTITY-BASED SECURITY

William D. Ivancic, NASA Glenn Research Center, Cleveland, Ohio

Abstract

Current telecommunications systems have very good security architectures that include authentication and authorization as well as accounting. These three features enable an edge system to obtain access into a radio communication network, request specific Quality-of-Service (QoS) requirements and ensure proper billing for service. Furthermore, the links are secure. Widely used telecommunication technologies are Long Term Evolution (LTE) and Worldwide Interoperability for Microwave Access (WiMAX)

This paper provides a system-level view of network-centric operations for the Global Airspace System (GAS) and the problems and issues with deploying new technologies into the system. The paper then focuses on applying the basic security architectures of commercial telecommunication systems and deployment of federated Authentication, Authorization and Accounting systems to provide a scalable, evolvable reliable and maintainable solution to enable a globally deployable identity-based secure airspace system.

Background

The air transportation community is continually looking to improve the safety and efficiency of the Global Airspace System (GAS). This community consists of a variety of national and international government organizations, airlines, and equipment suppliers and manufacturers. In general they have the common goal stated above, but in practice each organization has different stakeholders with often conflicting bottom-line goals. For example: the Federal Aviation Administration (FAA) and European Organisation for the Safety of Air Navigation (EUROCONTROL) primary goal is safety of flight, safety of life. While this is also a goal of the airlines, they must meet this goal while remaining profitable. The International Civil Aviation Organization (ICAO) and the International Air Transport Association (IATA) cooperate to ensure interoperability of the GAS. Groups such as NASA are chartered to develop new technologies directed at improving the safety and efficiency of the GAS.

The FAA is the national aviation authority of the United States. It has authority to regulate and oversee all aspects of American civil aviation. The FAA's mission is to provide the safest, most efficient aerospace system in the world.

EUROCONTROL is the European Organisation for the Safety of Air Navigation. It is an international civil organization working for seamless, pan-European air traffic management. EUROCONTROL coordinates and plans air traffic control for all of Europe.

The International Civil Aviation Organization (ICAO), is an agency of the United Nations. It codifies the principles and techniques of international air navigation and fosters the planning and development of international air transport to ensure safe and orderly growth.

The International Air Transport Association (IATA) is a trade association of the world's airlines with membership of roughly 260 airlines. IATA's mission is to represent, lead and serve the airline industry. They work in a number of areas including policy, safety, environmental impact, security and simplifying business to improve efficiencies and save money.

In order to improve efficiencies and maintain safety two major programs have been created – one in the United States and another one in Europe. These are the Next Generation Air Transportation System (NextGen) in the United States and Single European Sky Air Traffic Management (ATM) Research (SESAR). NextGen is an Air Traffic Control (ATC) modernization program which uses sophisticated technologies and new flight procedures to reduce flight delays, flight times and aircraft fuel burn/emissions. One of the key technologies is Global Positioning System (GPS). GPS should enable planes

to fly closer together, take more direct routes and avoid delays caused by airport "stacking". SESAR is a collaborative project to completely overhaul European airspace and its air traffic management (ATM).

NASA's Airspace Operations and Safety Program (AOSP) creates technologies to help NextGen fulfill its promise. AOSP works with the FAA, industry and academic partners to conceive and develop NextGen technologies to improve the intrinsic safety of current and future aircraft. The Safe Autonomous Systems Operations (SASO) and Shadow Mode Assessment Using Realistic Technologies for the National Airspace System (SMART-NAS) projects are part of AOSP. SASO identifies and develops the maximum possible autonomous capabilities. The SMART-NAS Project will develop an air traffic management simulation capability to explore integration of alternative concepts, technologies and architectures within the National Airspace System. In support of SMART-NAS, NASA Glenn Research Center (GRC) is working with NASA Ames Research Center (ARC) on Networked ATM architectures and technologies. GRC has a testbed at Cleveland Hopkins Airport to support this effort with emphasis on surface communications.

Goals

Looking at all the programs that exist to improve safety and efficiency in the global airspace system, one quickly realizes that the keys to success are network-centric operations and improved situational awareness. One of the critical enablers is *"connected aircraft"*. Connectivity to the aircraft must be secure, reliable, and manageable globally.

Modernization Issues

Why is it so difficult to get new technologies deployed in the global airspace system?

Safety

The airline industry has an excellent safety record. In order to maintain public confidence in air travel, safety must be the top priority. Thus any new technologies or any changes to operational procedures must be proven to at least maintain the current level of safety if not improve it. This is not an easy matter and can be rather expensive in terms of both time and money. As a result, the industry is often looked at as being reactive rather than proactive.

The "Able" List

Assuming we can get past the safety issues, then the general problem with deploying new technologies is that they do not meet all the requirements of what we coin the *"Able List"*.

The Able List

- Adaptable
- Affordable
- Deployable
- Evolvable
- Global(able)
- Maintainable
- Manageable
- Reliable
- Scalable
- Securable

Adaptable: A technology that is not adaptable is not likely to be embraced due to a high probability of obsolescence.

Affordable: If the greatest technology in the world is not affordable, it will not be accepted by the airline industry. Remember, the airlines must make money to survive. This is one reason satellite communications is often not embraced. The cost of the conductivity versus the overall perceived payback is not considered justified by many.

Deployable: If one has to take an aircraft off-line, then the airline cannot generate revenue from that aircraft while the new technology is being integrated. Thus, integration should be done during normal maintenance with little additional out-of-service time.

Evolvable: Technologies must seamlessly integrate into existing systems and any upgrades must be easy to make. There is no flag day[1].

Global(able): Global scalability must be considered. Airplanes fly from one city to another and from one country to another. All operations must be smooth and seamless and be capable of global deployment – particularly when it comes to security solutions.

[1] A change which requires a complete restart or conversion of a sizable body of software or data and requires that updates be performed almost simultaneously across the entire system or network. It came into use when a massive change was made to the Multics time-sharing system to convert from the old ASCII code to the new one; this was scheduled for Flag Day (a US holiday), June 14, 1966.

Maintainable: One must easily be able to maintain a system once it is deployed.

Manageable: One must be able to easily manage a system in a cost-effective manner.

Reliable: The system must be reliable – particularly in the aerospace industry. Reliability affects safety, maintainability and cost.

Scalable: It is significantly more challenging to make systems work on a global scale than it is for small-scale deployment such as confined to an individual airport. Scalability is hard.

Securable: If one cannot secure the system to the scale of its intended deployment it is rendered useless.

An Integrated Communication, Navigation and Surveillance System

Figure 1 illustrates an example of an integrated communication, navigation and surveillance system for Aeronautics. Four major entities are shown here: FAA[2], Port Authority, airlines, and Public Internet and Entertainment Services (PIES). Not shown are Unmanned Air Vehicles (UAVs). How UAVs are handled is a subject for future consideration. These four entities represent four security domains. Perhaps, with the exception of PIES, each of these entities needs to interact and exchange information in order to provide system-wide situational awareness thereby enabling each entity to properly manage assets and resources with the overall goal of maintaining safety and improving efficiencies.

A fully connected aircraft communicates over a variety of systems owned and operated by various entities both public and private. These connections include High Frequency (HF) for oceanic, Automatic Dependent Surveillance - Broadcast (ADS-B), Very High Frequency (VHF) radios, Airport Mobile Access Communication System (AeroMACS), Gatelink, satellite systems such as Inmarsat and Iridium, and cellular systems.

In order to get a sense deployment relative to scalability, consider the AeroMACS deployment for the Port Authority versus AeroMACS deployment for air traffic control in ATC operations. With regard to the Port Authority, the AeroMACS system is entirely controlled by one entity, the Port Authority. Thus, the entire AeroMACS network including all security and QoS configurations are controlled by the Port Authority. The system does not have to scale beyond the airport in question. The AeroMACS Authentication, Authorization and Accounting (AAA) server can be local and does not have to share any information with any other systems. However, for the ATC AeroMACS deployment, the access into the system must scale to a global level and must handle network layer mobility as a single aircraft may fly throughout the global airspace landing at various airports in different countries. Thus, the aircraft is a system that roams using multiple service providers and wireless technologies. Authorization, access and service agreements[3] must be manageable and deployable on a global scale. Note, there is a similar need for authorization, access, and service agreements on a global scale for Gatelink, various satellite systems, cellular systems, and future wireless systems.

Globally Deployable, Identity-based Secure Airspace System

The remainder of this paper focuses on applying the basic security architectures of commercial telecommunication systems to provide an affordable, scalable, evolvable reliable, maintainable and manageable solution to enable a globally deployable identity-based secure airspace system.

Issues/Requirements

The following are the system requirements:

1) Seamless Global Access,
2) Seamless Billing,
3) Manageable Service Agreements (e.g. QoS),
4) Scalable Seamless Management,
5) Seamless Roaming, and
6) Single Identity.

In the above requirements, "seamless" implies machine-to-machine communications without human intervention. A single identity is the key to enabling seamless operations.

It is currently unclear how to implement the requirements above in the GAS. Fortunately, the telecommunication industry and in particular the Internet Engineering Task Force (IETF) and the 3rd

[2]EUROCONTROL or another air traffic management entity depending on where one is in a global deployment

[3]Quality of Service settings, often which vary depending on the service provider and wireless technology.

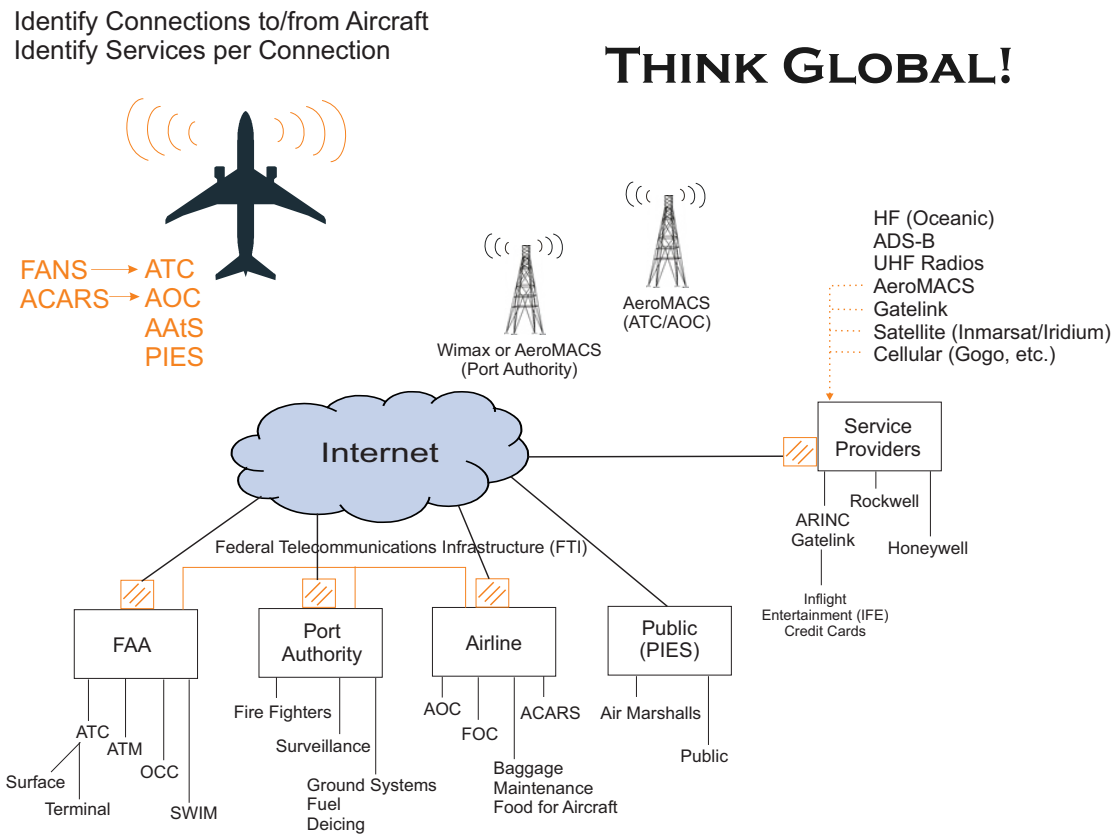

Figure 1. Integrated Communication, Navigation and Surveillance System

Generation Partnership Project (3GPP) have developed many standards and architectures to address most of these issues.

What is an Identity?

In this context, an identity is something that can be used to uniquely identify a system. For aeronautics, that system is an aircraft. Since the identity will be used to gain access into an aeronautical network and for billing, we must be able to authenticate that identity and ensure it is not spoofed. We also desire that an identity is usable across multiple access systems.

In commercial systems there are two basic methods used to identify a system: Certificates or some form of serial number such as an electronic serial number (ESN) or international mobile equipment identity (IMEI). ESNs and IMEIs are used by the cell phone industry. One problem with ESNs and IMEIs is that they are assigned to a specific piece of hardware making portability an issue. A solution to this is the Subscriber Identification Module (SIM), an integrated circuit that securely stores the International Mobile Subscriber Identity (IMSI) number and its related key which are used to identify and authenticate subscribers on mobile telephony devices. SIM cards are designed to be transferable between different mobile devices. If a piece of equipment breaks or is upgraded, one can simply move the SIM card to the replacement unit and it becomes operational again. No reregistration needs to occur.

An identity certificate or digital certificate is an cryptographic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the entity examining the certificate trusts the signer, then they know they can use that key to communicate with its owner. Identity certificates are

associated with the Public Key Infrastructure (PKI) and usually associate with X.509, an International Telegraph Union - Telecommunication standardization sector (ITU-T) standard for a public key infrastructure [1][2].

Certificate Management in Aeronautical Systems

Certificate management is difficult in any system even a single owner system. Regarding aeronautics, in order to be scalable, manageable and affordable, a single identity (a single certificate) is highly desirable. It may be possible to map other certificates to this single identity in order to utilize that single identity across multiple systems owned and operated by different service providers.

In aeronautics systems, various wireless systems have vastly different bandwidth capabilities. Likewise, various certificates and keys have vastly different bandwidth requirements. Harmonizing these is a challenge. The FAA sponsored a report on AeroMACS privacy key management [3]. Within this report it was determined that specifying the operation of Authentication, Authorization and Accounting (AAA) capabilities was out-of-scope. It was agreed that the Minimum Operational Performance Specification (MOPS) should address the air interface between the subscriber station and the base station with some material to address interoperability with AAA sites (e.g., an interoperable certificate profile). However, Key management and synchronization across all AAA sites was determined to be a ground AeroMACS deployment issue. Some important points from this document follow:

- Key pairs and the corresponding certificates for airborne users are associated with a given airframe, and not, for example, with a pilot or a particular flight identifier. In addition, key pairs and certificates are not assigned to individual pieces of equipment on an airframe.
- ICAO Doc 9880 Part IVB specifies a Certificate Authority (CA) architecture in which each State operates (or contracts with an entity to operate on its behalf) a root-level CA. These State CAs have a non-transitive peer relationship amongst one another rather than a hierarchical relationship. The relationship among such CAs is expected to be established and maintained through bilateral and/or multilateral agreements, which includes, for example, provision for cross-certification.
- Harmonization amongst the AeroMACS and Aeronautical Telecommunication Network (ATN) based security solutions is to minimize the cryptographic infrastructure implemented on an airframe. Harmonizing these solutions will allow airframe and avionics manufacturers to use common toolsets to provide security services for multiple applications. The areas of harmonization are the underlying cryptographic settings, certificate content, and CA architecture.
- Provisioning must occur across ATN Open System Interconnection (OSI) Security, ATN Internet Protocol Suite (IPS) Security, Aeronautical Radio, Incorporated (ARINC) 823, WiMAX and AeroMACS

Quality of Service

Quality of service (QoS) is the overall performance of a service as seen by the users of the network. QoS has numerous characteristics including error rates, bit rate, throughput, transmission delay, availability, and jitter. Different services require different QoS. For example, voice may be able to withstand a high error rate but requires low transmission delay whereas a file transfer may require relatively low error rates but can withstand jitter, transmission delay, and operate over a variety of bit rates. Video may require low error rates, low jitter, and high bit rate. The specification of QoS service parameters is known as a service flow. Per service flow QoS is the ability to identify a traffic flow and enable rules on how that specific flow should be treated including how the flow should behave when forwarded with other traffic flows.

In order to be scalable and manageable, one must be able to specify QoS for a particular entity globally. The QoS specifications are likely to vary per link type (e.g. AeroMAX, Gatelink, Satellite, 4G/5D), but should not vary per service provider for any particular link type. This implies some type of roaming agreements between service providers for any particular link type.

System Access and QoS Provisioning

In order to understand concepts of system access and QoS provisioning, we will examine two existing systems: Gatelink[4] and LTE.

System Access

First, we will summarize the Gatelink access methodology as described in the ARINC specification 822 [4] illustrated in figure 2 When the aircraft is in range of the airport Access Point (AP), the aircraft client will scan for available APs. Once the Radio Frequency (RF) association has completed, the aircraft will initiate an authentication session with the airport AP based on the registered aircraft (Terminal Wireless LAN Functions (TWLF)) and the AAA server. That server could be at the airport, or at the airline under the Network Administrator's control as shown in figure 2. For global scalability, the AAA server should be at the airline in which case, the AP would also need a Remote Authentication Dial-In User Service (RADIUS) proxy capability[5]. Proxy service enables a RADIUS/AAA server to forward an authentication request from a local server to a remote RADIUS server and return the remote server's reply to the local server. In this way, client/server architecture is established between local and remote servers in effect, extending the wireless link from the aircraft to the airline's network.

An X.509 certificate is used to gain access to the system[6]. The X.509 certificate must be signed by a valid certificate authority and must be installed on each Gatelink client (aircraft). The AAA server will acknowledge or deny the signature of the root authority or will forward the authentication requests to the airline or some authorized third party RADIUS server via proxy depending on the agreement with the airline. The remote RADIUS server will acknowledge or deny the request.

If the accessing system (or user) is not in the local RADIUS server configurations, the server will look for a realm name and pass the authentication request to a remote RADIUS server which is mapped via manual configuration to the realm name.

The Access System (User-Name) RADIUS attribute is a character string that typically contains the accessing system account's location (called the realm) and the accessing system account's name. The realm is synonymous with the concept of domain, including Domain Name System (DNS) domains and Active Directory® domains. For example, in the URL http://www.ABCXYZ.com/index.html, the domain name is ABCXYZ.com. which is also the realm name.

Internationalized Domain Names (IDNs) may be included in certificates and Certificate Revocation Lists (CRLs) in the subjectAltName and issuerAltName extensions, name constraints extension, authority information access extension, subject information access extension, CRL distribution points extension, and issuing distribution point extension [5].

Realm names are configured in connection request policies while designing and deploying the RADIUS infrastructure to ensure that connection requests are routed from RADIUS network access servers (AAA airport server in figure 2), to remote distributed RADIUS servers (Airline Network AAA server) that can authenticate and authorize the connection request.

Decentralizing AAA has multiple problems that must be considered. These problems mainly relate to user account integrity, user profile management, failover mechanisms, and AAA interworking for roaming users [6]. Other considerations for connected aircraft are acquisition time (the time it takes to get authorization, QoS parameters and IP connectivity to remote AAA systems).

Multi-Domain System Access

Figure 3 is from a Cisco White paper, Architecture for Mobile Data Offload over Wireless Fidelity (Wi-Fi) Access Networks [7]. This illustrates the relationship between a Third Generation (3G) Radio Access Network (RAN), an LTE RAN service provider and a cooperating Wi-Fi service provider. When a system wishes to connect to the Wi-Fi RAN, authentication can be setup such that the AAA server at the Wi-Fi Internet Service Provider (ISP) proxies to the 3G/LTE Service Provider (SP) network access system. This allows a non-3GPP Internet Protocol (IP)

[4]We use the Gatelink illustration as Gatelink does not require and QoS management and is therefore a simpler example.

[5]There needs to be a method of securing the proxy transaction between the airport and airline, because the current RADIUS proxy protocol is not secure.

[6]It is highly desirable to have one certificate for Gatelink, AeroMACS, WiMAX, Satellite Communications (SATCOM), LTE, etc. in order to scale globally and be manageable.

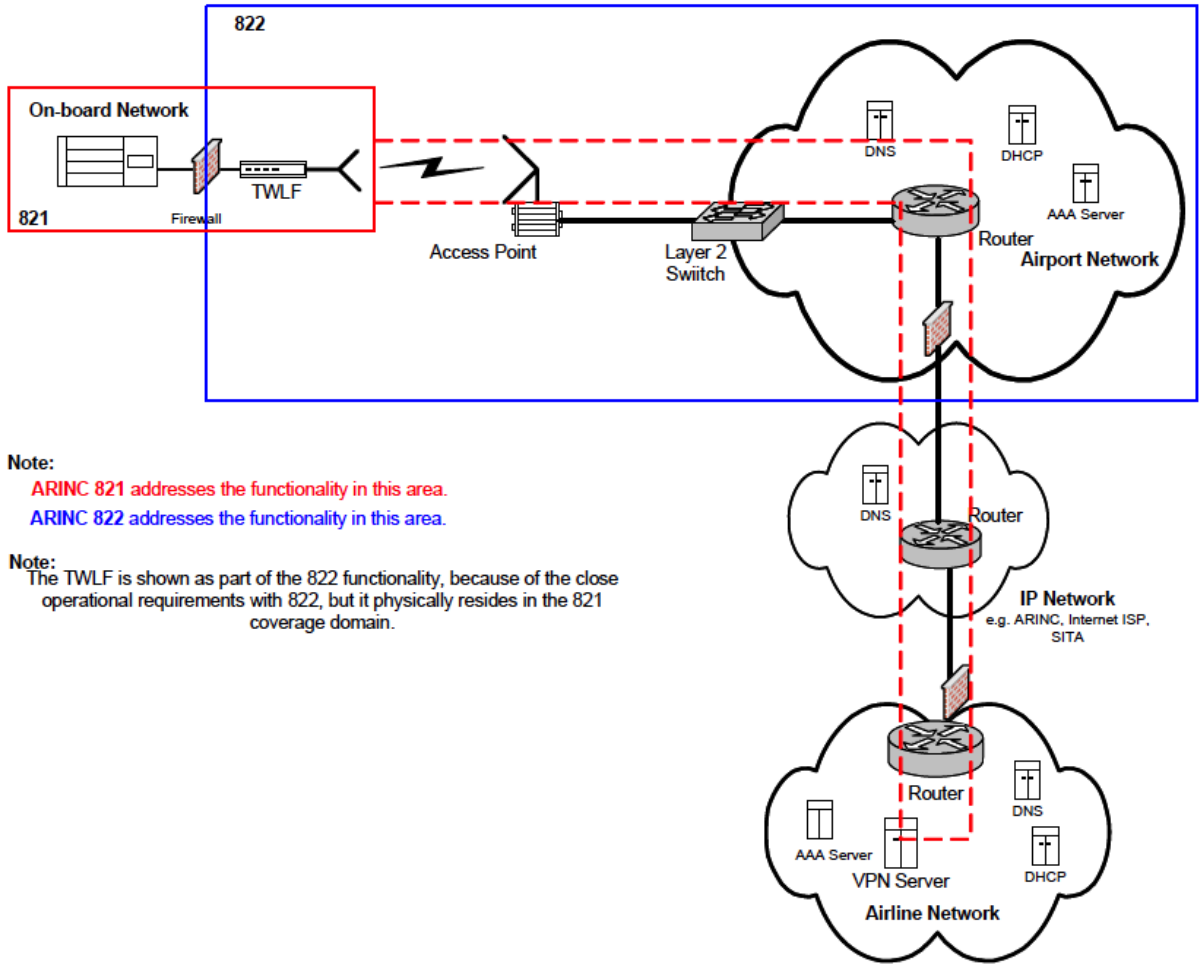

Figure 2. Gatelink Network Architecture Recommendations and Concept of Operations [4]

access into the 3G Mobile Packet Core (MPC). Note, the Policy and Change Control (PCC) is managed by the 3G/LTE Service Provider. The PCC is where QoS is managed in the 3GPP network architecture.

To control subscriber access to Wi-Fi networks, multiple authentication methods can be used. In a typical modern Wi-Fi network, two types of authentication are available. The first method, portal based authentication, targets customers without a permanent contract with the operator (vouchers, time-limited access,Short Message Service (SMS) payments, etc.). Alternatively, Extensible Authentication Protocol (EAP) authentication provides transparent and easy access for the subscribers with SIM cards or certificates[7]. EAP-based authentication allows transparent authentication and secure communication without interaction from the subscriber (only initial configuration of the Service Set ID (SSID) which, for Gatelink, is predefined and configured in the TWLF [4].

For an aeronautic global network, visualize the Wi-Fi access as Gatelink, the 3G as AeroMACS and LTE as a future wireless access.

QoS Provisioning

For all practical purposes, an aircraft could be considered constantly roaming across multiple wireless networks owned and operated by multiple entities. How one manages QoS over such a diverse network is an interesting challenge. Fortunately, it is not unique to the aeronautics industry. The commercial telecommunication and ISPs have had to address this

[7]EAP authentication would be use for aeronautics.

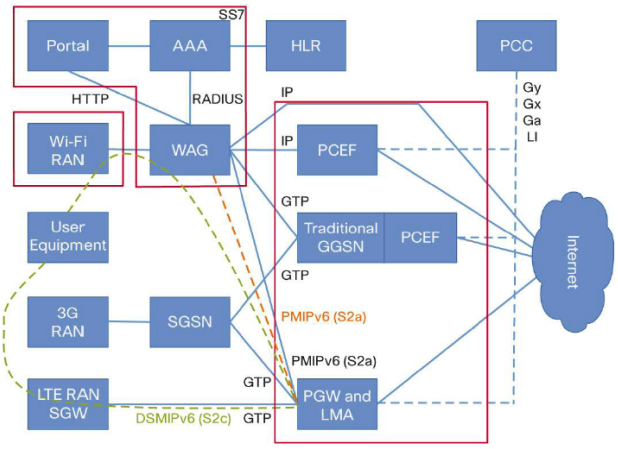

Figure 3. Multi-Domain System Access [7]

exact problem.

Figure 4, PCC reference architecture for fixed Broadband Access Interworking (visited access), illustrates how QoS and policy is provisioned in a roaming system for a 3GPP network. Regarding QoS provisioning, the important interface is the S9 reference point. "S9 resides between a Policy and Charging Rules Function (PCRF) in the Public Land Mobile Network (PLMN) Home PLMN (H-PLMN) (H-PCRF) and a PCRF in the Visiting PLMN (V-PLMN) (V-PCRF). For roaming with a visited access, this interface reference enables the Home PCRF (H-PCRF) to:

- Have dynamic PCC control, including the Policy and Charging Enforcement Function (PCEF) and, if applicable, Bearer Binding and Event Reporting Function (BBERF), and, if applicable, Traffic Detection Function (TDF), in the V-PLMN;
- Deliver or receive IP Connectivity Access Network (CAN) specific parameters from both the PCEF and, if applicable, BBERF, in the V-PLMN;
- Serve recieve authorizations and event subscriptions from an Application Function (AF) in the V-PLMN;
- Receive application identifier, service data flow descriptions, if available, application instance identifiers, if available, and application detection start/stop event triggers report.

For roaming with a home routed access, the S9 interface enables the H-PCRF to provide dynamic QoS control policies from the H-PLMN, via a Visiting PCRF (V-PCRF), to a BBERF in the V-PLMN [8]."

The LTE PCC functions include:

- **Policy and Charging Rules Function (PCRF)** The PCRF provides policy control and flow based charging control decisions.
- **Policy and Charging Enforcement Function (PCEF)** The PCEF is implemented in the serving gateway, this enforces gating and QoS for individual IP flows on behalf of the PCRF. It also provides usage measurement to support charging.
- **Online Charging System (OCS)** The OCS provides credit management and grants credit to the PCEF based on time, traffic volume or chargeable events.
- **Off-line Charging System (OFCS)** The OFCS receives events from the PCEF and generates Charging Data Records (CDR) for the billing system.

The WiMAX Policy and Change Control architecture is very similar to 3GPP as shown if figure 5. The Access Service Network (ASN) in WiMAX maps to the RAN in 3GPP while the interface between the Visiting Connection Service Network (CSN) (vCSN) and Home CSN (hCSN) is nearly equivalent to interface reference point S9 in figure 4.

WiMAX[8] and 3GPP LTE have been designed with different QoS frameworks and means to enable QoS support for evolving Internet applications. Network initiated or client initiated QoS are both supported in IEEE 802.16e/IEEE 802.16m systems. Both operator managed service and unmanaged service can be supported. This flexible architecture gives the mobile client opportunities for differentiation. In contrast, LTE only supports network initiated QoS control [10].

LTE QoS

3rd Generation Partnership Project LTE have been designed with a QoS framework to support QoS of evolving Internet applications. LTE offers two types of bearers (classes): Guaranteed Bit Rate (GBR) and non-Guaranteed Bit Rate. GBR is similar to Unsolicited Grant Service (UGS) in

[8]Note, AeroMACS is a tailored instance of WiMAX and uses the same architecture and protocols. As such, AeroMACS implements QoS management in the same manner as WiMAX.

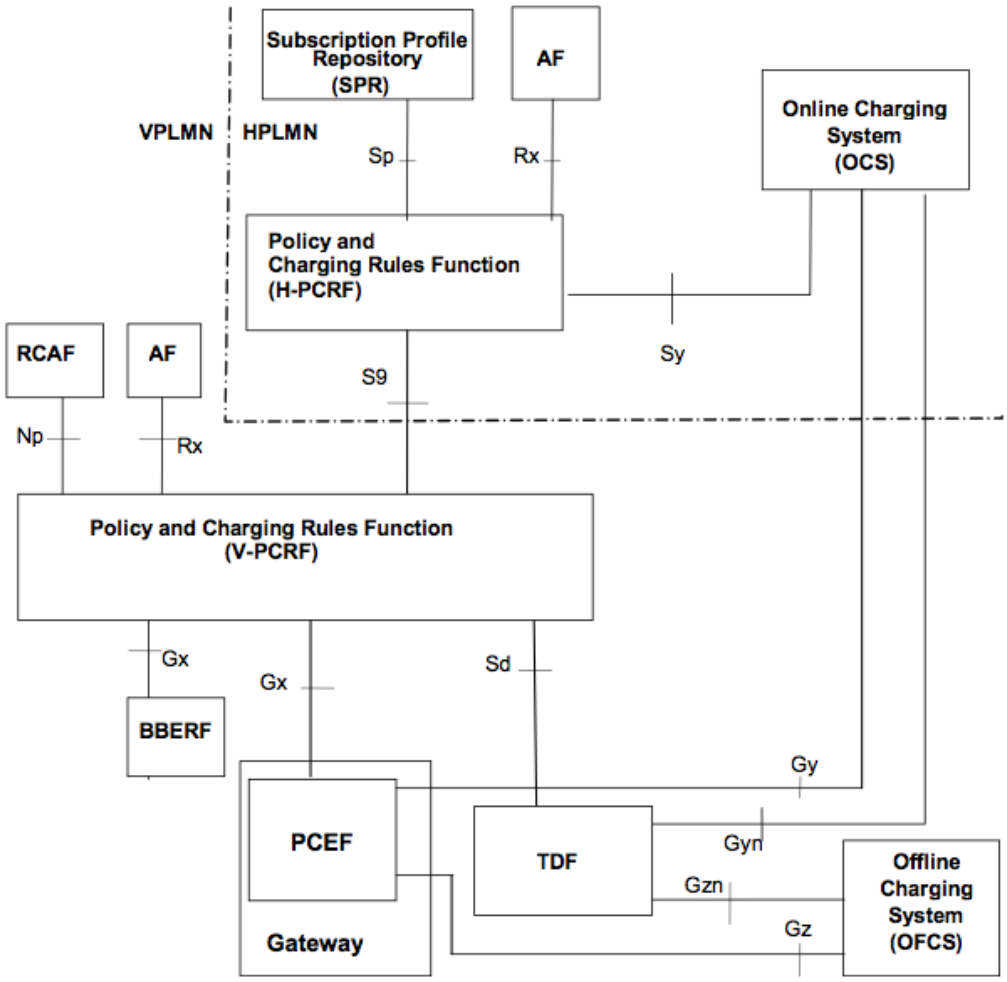

Figure 4. PCC Reference architecture for Fixed Broadband Access Interworking (visited access) [8]

WiMAX/AeroMACS. Resources related to a GBR value associated with the bearer are permanently allocated when a bearer becomes established or modified. A non-GBR bearer is the default bearer. A service utilizing a non-GBR bearer may experience congestion-related packet loss [11].

> "The QoS level of granularity in the LTE Evolved Packet System (EPS) is a packet flow established between the packet data network gateway and the user terminal, the bearer channel. The traffic running between a particular client application and a service can be differentiated into separate Service Data Flows (SDFs). SDFs mapped to the same bearer channel receive a common QoS treatment (e.g., scheduling policy, queue management policy, rate shaping policy, Radio Link Control (RLC) configuration). Each SDF is associated with one and only one QoS Class Identifier (QCI). For the same IP CAN session, multiple SDFs with the same QCI and Allocation and Retention Priority (ARP) can be treated as a single traffic aggregate which is referred to as an SDF aggregate. Each QCI maps to specific applications. QCI characteristics describe the packet forwarding treatment that an SDF aggregate receives edge-to-edge between the User Equipment (UE) and the PCEF in terms of the following performance characteristics:
>
> 1) Resource Type (GBR or Non-GBR);

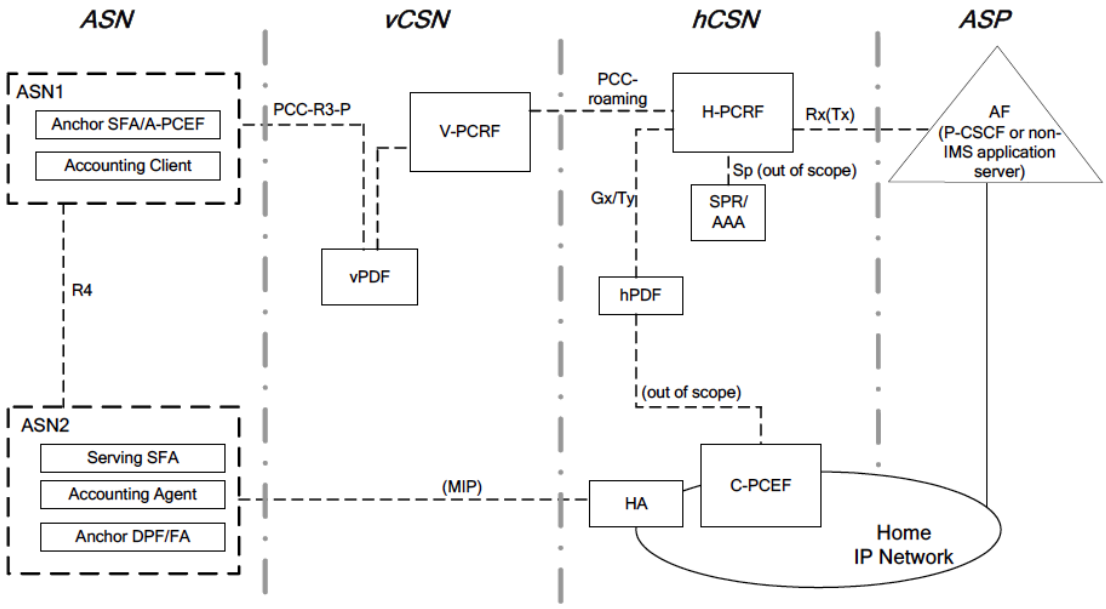

Figure 5. WiMAX Policy Control architecture – roaming scenario with HA in the home network [9]

2) Priority;
3) Packet Delay Budget;
4) Packet Error Loss Rate [10]."

"The Policy and Change Control (PCC) function in LTE networks brings together and enhances capabilities from earlier 3GPP releases to deliver dynamic control of policy and charging on a per subscriber and per IP flow basis. The LTE Evolved Packet Core (EPC) includes a PCC architecture that provides support for fine-grained QoS and enables application servers to dynamically control the QoS and charging requirements of the services they deliver. It also provides improved support for roaming. Dynamic control over QoS and charging will help operators monetize their LTE investment by providing customers with a variety of QoS and charging options when choosing a service [12]."

WiMAX QoS

Five types of scheduling services have been defined for the WiMAX airlink corresponding to the traffic characteristics of different services:

- Unsolicited Grant Service (UGS),
- real-time Polling Service (rtPS),
- non-real-time Polling Service (nrtPS),
- extended-real-time Polling Service (ertPS) and
- Best Effort (BE).

UGS, rtPS and ertPS are mainly used for real-time traffic and interactive traffic such as Voice-Over-IP (VoIP), video and online gaming, while nrtPS and BE are usually utilized for non-real-time traffic such as file transfers, emails, and web browsing.

Each service class has a myriad of QoS parameters associated with uplink/downlink scheduling for a service flow (e.g. Maximum sustained rate, Maximum reserved traffic rate, Maximum latency, Jitter tolerance, Packet loss, throughput) [13].

Traffic classification and mapping from application packets onto Service Flows (SFs) in WiMAX is done at the convergence sublayer (CS). Classification is often done using a five-tuple, such as source and destination IP addresses, source and destination port address, protocol, and Differentiated Services Code Point (DSCP) [14].

During the creation of a SF, the CS that the connection will use is defined. Possible choices of CS are No CS, Packet IPv4, Packet IPv6, Packet

802.3/Ethernet, Packet 802.1Q VLAN[9], Packet IPv4 over 802.3/Ethernet, Packet IPv6 over 802.3/ Ethernet, Packet IPv4 over 802.1Q VLAN, Packet IPv6 over 802.1Q VLAN and Asynchronous Transfer Mode [10].

Initial Network Access Example for WiMAX

To clarify and simplify understanding of network access, a simple WiMAX example is provided. Figure 6 shows the reference architecture for providing service to a roaming Mobile Station (MS) with usage of the Home Agent (HA) in the visited CSN. Authentication, authorization as well as policy information (the QoS profile) is provided from the home CSN to the visited CSN over the reference point R5. Accounting information is forwarded from the visited CSN to the home CSN over R5, and access to services in the home CSN may also be provided over R5 whereas Internet access is usually established directly out of the visited CSN. Note, it is possible and a valid configuration to be roaming with the HA located in the home Network Service Provider (NSP) [15].

Authentication, Authorization and Accounting (AAA) Servers

The AAA server, QoS management, the Policy Function (PF) and Policy and Change Control (PCC) are key elements of any of the modern telecommunication architectures. These functions are often performed using a Remote Authentication Dial-In User Service (RADIUS) [16] or Diameter [17] server.

The RADIUS protocol carries authentication, authorization and configuration information between a Network Access Server (NAS) and a RADIUS authentication server. Requests and responses carried by the RADIUS protocol are called RADIUS attributes. These attributes can be username, Service-Type, and so on. These attributes provide the information needed by a RADIUS server to authenticate users and to establish authorized network service for them. The RADIUS protocol also carries accounting information between a NAS and a RADIUS accounting server [18].

[9]IEEE 802.1Q standard defines a system of tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames. The standard also contains provisions for a quality of service prioritization scheme.

The RADIUS-Based Policing feature enables the PCEF in the access network to make automatic changes to the policing rate of specific sessions and services. Policies can be based on any attribute in a request or response, include checking both the existence of (or lack of) an attribute, and the contents of an attribute. They can filter out attributes, or re-write the contents of attributes. Attributes can be created, deleted, or edited in a policy. Policies can leverage information in Structured Query Language (SQL), Lightweight Directory Access Protocol (LDAP), flat-text files, or any other source of data. Policies can be based on identities (user, group, or role), location (client IP, port, etc.), time (date, time of day), authentication method (Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), EAP type, etc.), or any other piece of information that is in a RADIUS packet or in a database. Policies can enforce Virtual Local Area Network (VLAN) capabilities, filtering QoS, etc. [19].

Authentication, Authorization and Accounting (AAA) protocols such as RADIUS were initially deployed to provide dial-up Point-to-Point Protocol (PPP) and terminal server access. Over time, AAA support was needed on many new access technologies as the scale and complexity of AAA networks grew. AAA was also used on new applications (such as VoIP). This led to new demands on AAA protocols. As a result, Diameter[10] was developed – evolving from and replacing the much less capable RADIUS protocol. *Diameter is not directly backwards compatible but provides an upgrade path for RADIUS.*

The new network access requirements for AAA protocols addressed by Diameter are summarized below.

- Failover
- Transmission-level security – RADIUS support for IPsec is not required.
- Reliable transport – RADIUS runs over UDP, and does not define retransmission behavior; as a result, reliability varies between implementations.
- Agent support – RADIUS does not provide for explicit support for agents, including proxies, redirects, and relays. Since the expected behavior

[10]The name is a play on words, derived from the RADIUS protocol. A diameter is twice the radius.

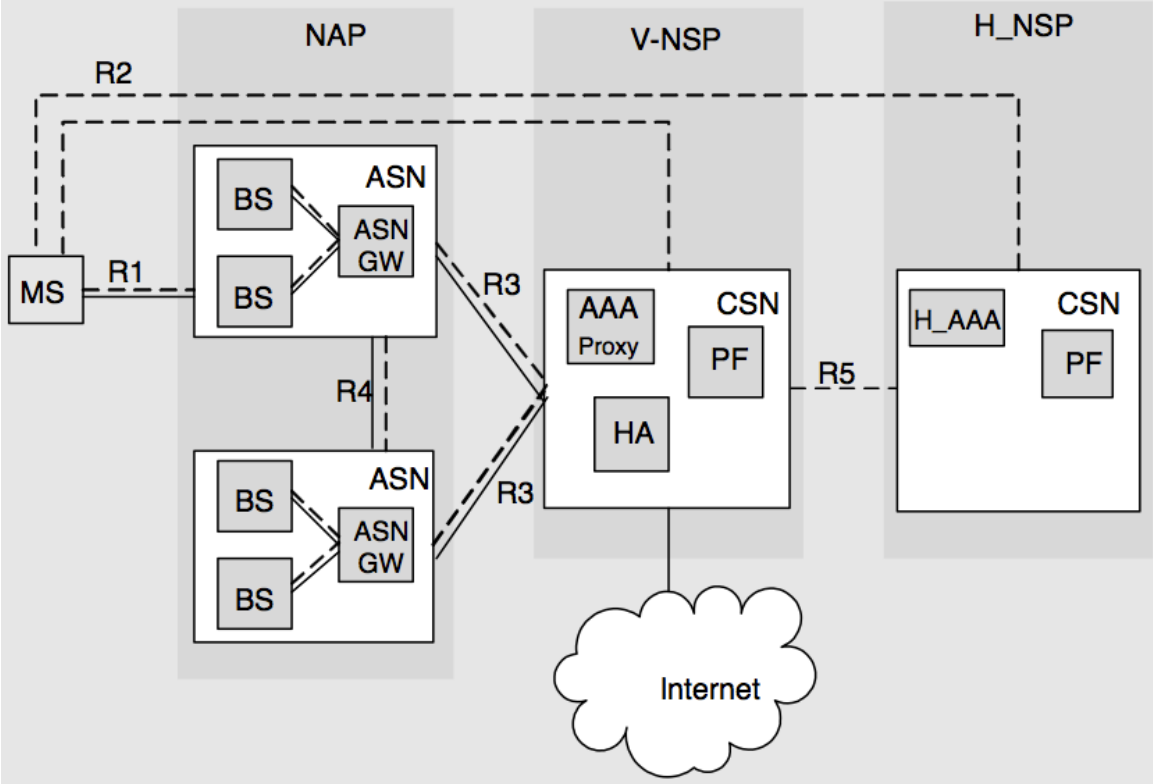

Figure 6. WiMAX Roaming with HA located in the visited NSP [15]

is not defined, it varies between implementations.

- Server-initiated messages
- Transition support – Considerable effort has been expended in enabling backward compatibility with RADIUS so that the two protocols may be deployed in the same network.
- Capability negotiation
- Peer discovery and configuration – RADIUS implementations typically require that the name or address of servers or clients be manually configured, along with the corresponding shared secrets. This results in a large administrative burden and creates the temptation to reuse the RADIUS shared secret, which can result in major security vulnerabilities if the Request Authenticator is not globally and temporally unique as required in RFC2665 [16].

Over time, the capabilities of Network Access Server (NAS) devices have increased substantially. As a result, Diameter is a considerably more sophisticated protocol than RADIUS Through the use of extensions, the protocol was designed to be extensible to support proxies, brokers, strong security, mobile IP, network-access servers, accounting and resource management.

Summary

In order to globally deploy new communications technologies into the Global Airspace System (GAS) those technologies must meet all the requirements of the “Able List”. The GAS currently consists of a variety of communications links, often quite old such as VHF analog radios with limited bandwidth capability. New technologies such as Gatelink and AeroMACS offer greater capability, greater bandwidth, better security and potential cost savings. However, these systems will not be deployed if the cost of deployment and management outweighs the benefits. Identity-based security with single certificate sign-on for system access along with the capability of managing QoS policy for diverse systems in a centralized location has the potential to ensure a smooth, evolvable, scalable, manageable, affordable deployment. Modern telecommunications networks have shown this to be possible for single communi-

cation technologies types (e.g. LTE and WiMAX). In addition the tools, protocols and architectures exist. The outstanding question remains: *"Can a single identity and centralized QoS policy management be deployed that encompasses multiple Access Service Networks and Network Service Providers to enable connected aircraft?"*

References

[1] I. Recommendation, "509 (2005)| iso/iec 9594-8: 2005," *Information technology–Open Systems Interconnection–The Directory: Public-key and attribute certificate frameworks*,

[2] C. Adams, S. Farrell, T. Kause, and T. Mononen, "Internet x.509 public key infrastructure certificate management protocol (cmp)," Internet Engineering Task Force, RFC 4210, Sep. 2005. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4210.txt.

[3] I. Exelis, "New atm requirements – future communications, c-band and l-band communications study aeromacs privacy key management report," FAA, Final Report SE2020 TO 0008 (TORP 1240) Task 3.2 Contract DTFAWA-10-D-00028, 2012.

[4] "Aircraft / ground aircraft / ground ip communication (gatelink)," ARINC, Tech. Rep. ARINC SPECIFICATION 822-1, 2008.

[5] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile," Internet Engineering Task Force, RFC 5280, May 2008. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5280.txt.

[6] D. Forsberg, "Secure distributed aaa with domain and user reputation," in *World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE International Symposium on a*, IEEE, 2007, pp. 1–6.

[7] "Architecture for mobile data offload over wi-fi access networks," Cisco System, White Paper C11-701018-00, 2012. [Online]. Available: http://tools.cisco.com/search/results/display?url=http%3a%2f%2fwww.cisco.com%2fc%2fen%2fus%2fsolutions%2fcollateral%2fservice-provider%2fservice-provider-wi-fi%2fwhite_paper_c11-701018.pdf&pos=1&query=C11-701018-00.

[8] 3GPP, "Policy and charging control architecture," 3GPP, Technical Specification 3GPP TS 23.203, 2015. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/23_series/23.203/23203-d40.zip.

[9] "Architecture, detailed protocols and procedures policy and charging control," WiMAX Forum, Tech. Rep. WMF-T33-109-R015v02, 2010.

[10] M. Alasti, B. Neekzad, J. Hui, and R. Vannithamby, "Quality of service in wimax and lte networks [topics in wireless communications]," *Communications Magazine, IEEE*, vol. 48, no. 5, pp. 104–111, 2010.

[11] H. Ekström, "Qos control in the 3gpp evolved packet system," *Communications Magazine, IEEE*, vol. 47, no. 2, pp. 76–83, 2009.

[12] 2015. [Online]. Available: http://lteworld.org/ltefaq/how-does-policy-control-and-charging-works-lte.

[13] *Wimax technology for broadband wireless access - 7.4*, August. [Online]. Available: http://etutorials.org/Networking/wimax+technology+broadband+wireless+access/Part+Three+WiMAX+Multiple+Access+MAC+Layer+and+Qos+Management/Chapter+7+Convergence+Sublayer+CS/7.4+CS+and+QoS/.

[14] F. Baker, J. Polk, and M. Dolly, "A differentiated services code point (dscp) for capacity-admitted traffic," Internet Engineering Task Force, RFC 5865, May 2010. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5865.txt.

[15] "Stage 2: Architecture tenets, reference model and reference points," WiMAX Forum, Tech. Rep. WMF-T32-002-R010v04, 2009.

[16] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote authentication dial in user service (radius)," Internet Engineering Task Force, RFC 2865, Jun. 2000. [Online]. Available: http://www.rfc-editor.org/rfc/rfc2865.txt.

[17] V. Fajardo, J. Arkko, J. Loughney, and G. Zorn, "Diameter base protocol," Internet Engineering Task Force, RFC 6733, Oct. 2012. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6733.txt.

[18] *Configuring radius-based policing*, August. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/isg/configuration/xe-3s/isg-xe-3s-book/isg-radius-pol.html#GUID-1CDFAA27-177E-42F7-AD9F-05A17248526D.

[19] 2015. [Online]. Available: http://freeradius.org/features/policy.html.

Acronyms List

3G Third Generation
3GPP 3rd Generation Partnership Project
AAA Authentication, Authorization and Accounting
ADS-B Automatic Dependent Surveillance - Broadcast
AeroMACS Airport Mobile Access Communication System
AF Application Function
ARC Ames Research Center
AOSP Airspace Operations and Safety Program
ARINC Aeronautical Radio, Incorporated
ARP Allocation and Retention Priority
ASN Access Service Network
ATC Air Traffic Control
ATM Air Traffic Management
ATN Aeronautical Telecommunication Network
AP Access Point
BBERF Bearer Binding and Event Reporting Function
BE Best Effort
CA Certificate Authority
CAN Connectivity Access Network
CDR Charging Data Records
CHAP Challenge-Handshake Authentication Protocol
CRL Certificate Revocation List
CS convergence sublayer
CSN Connection Service Network
DNS Domain Name System
DSCP Differentiated Services Code Point
EAP Extensible Authentication Protocol
EPC Evolved Packet Core
EPS Evolved Packet System
ertPS extended-real-time Polling Service
EUROCONTROL European Organisation for the Safety of Air Navigation
FAA Federal Aviation Administration
GAS Global Airspace System
GBR Guaranteed Bit Rate
GPS Global Positioning System
GRC Glenn Research Center
HA Home Agent
hCSN Home CSN
HF High Frequency
H-PCRF Home PCRF
H-PLMN Home PLMN
IATA International Air Transport Association
ICAO International Civil Aviation Organization
IDN Internationalized Domain Name
IETF Internet Engineering Task Force
IPS Internet Protocol Suite
IP Internet Protocol
ISP Internet Service Provider
ITU-T International Telegraph Union - Telecommunication standardization sector
LDAP Lightweight Directory Access Protocol
LTE Long Term Evolution
MOPS Minimum Operational Performance Specification
MPC Mobile Packet Core
MS Mobile Station
NAS Network Access Server
NASA National Aeronautics and Space Administration
NextGen Next Generation Air Transportation System
nrtPS non-real-time Polling Service
NSP Network Service Provider
OCS Online Charging System
OFCS Off-line Charging System
OSI Open System Interconnection
PAP Password Authentication Protocol
PCC Policy and Change Control
PCEF Policy and Charging Enforcement Function
PCRF Policy and Charging Rules Function
PF Policy Function
PIES Public Internet and Entertainment Services
PKI Public Key Infrastructure
PLMN Public Land Mobile Network
PPP Point-to-Point Protocol
QCI QoS Class Identifier
QoS Quality-of-Service
RADIUS Remote Authentication Dial-In User Service
RAN Radio Access Network
RF Radio Frequency
RLC Radio Link Control
rtPS real-time Polling Service
SASO Safe Autonomous Systems Operations

SATCOM Satellite Communications
SDF Service Data Flow
SESAR Single European Sky ATM Research
SF Service Flow
SIM Subscriber Identification Module
SMART-NAS Shadow Mode Assessment Using Realistic Technologies for the National Airspace System
SMS Short Message Service
SP Service Provider
SQL Structured Query Language
SSID Service Set ID
TDF Traffic Detection Function
TWLF Terminal Wireless LAN Functions
UAV Unmanned Air Vehicle
UE User Equipment
UGS Unsolicited Grant Service
vCSN Visiting CSN
VLAN Virtual Local Area Network
V-PCRF Visiting PCRF
V-PLMN Visiting PLMN
VHF Very High Frequency
VoIP Voice-Over-IP
Wi-Fi Wireless Fidelity
WiMAX Worldwide Interoperability for Microwave Access